

1 Claims:

2 1. A proxy server for relaying communications between
3 applications and for performing an additional process
4 comprising:

5 a key manager for managing multiple keys used to
6 generate a digital signature to be provided for a message
7 document that is exchanged between said applications;

8 a signature key determiner for extracting said message
9 document from a predetermined application, and for, based on
10 said message document, determining a key used to provide a
11 digital signature; and

12 a signature generator for providing a digital signature
13 for said message document by using said key that is obtained
14 from said key manager based on a determination made by said
15 signature key determiner, and for transmitting said message
16 document with said digital signature to a destination
17 application.

18 2. The proxy server according to claim 1, wherein said key
19 manager sets multiple key selection rules for obtaining said
20 key, and only when said key selection rules are satisfied
21 can said signature generator obtain said key.

22 3. The proxy server according to claim 2, wherein, when
23 said key for generating a digital signature for said message
24 document can not be obtained, said signature generator
25 employs a replacement key that is defined in advance to
26 provide a digital signature.

1 4. The proxy server according to claim 3, wherein, after
2 said signature generator has provided a digital signature
3 using said replacement key, when said acquisition condition
4 that is determined for the original key based on said
5 message document is satisfied to enable the acquisition of
6 said original key, said signature generator again provides a
7 digital signature using said original key.

8 5. The proxy server according to claim 1, further
9 comprising:

10 a log manager for storing said message document with a
11 digital signature provided by said signature generator, and
12 for managing a log.

13 6. The proxy server according to claim 4, wherein said log
14 manager stores not only said message document for which said
15 signature generator has provided a digital signature using
16 said replacement key, but also said message document without
17 digital signature; and wherein said signature generator
18 obtains, from said log manager, said message document
19 without said digital signature, and provides a digital
20 signature using said original key.

21 7. A digital signature system comprising:

22 applications for performing data processing; and
23 a proxy server connected to said applications via a
24 network,

25 wherein said proxy server intercepts a communication,
26 transmitted through said network, from an application to an

1 external destination device, provides a digital signature
2 for a message document exchanged via said communication, and
3 transmits said message document with said digital signature
4 to said external destination device.

5 8. The digital signature system according to claim 7,
6 wherein said proxy server permits a key used to provide a
7 digital signature to be changed in accordance with the
8 contents of a message document; and wherein said proxy
9 server sets key selection rules for said key and permits
10 digital signature using said key when said key selection
rules have been satisfied.

11
12 9. The digital signature system according to claim 8,
13 wherein, when said key selection rules for said key used to
14 provide a digital signature for said message document have
15 not been satisfied, said proxy server employs a
16 predetermined replacement key to provide a digital
17 signature; and wherein, when said key selection rules for
18 said key are satisfied after said digital signature has been
19 provided using said replacement key, said proxy server again
20 employs said key to provide a digital signature for said
21 message document.

22 10. A digital signature verification system comprising:
23 applications for performing data processing; and
24 a proxy server connected to said applications via a
25 network,
26 wherein said proxy server intercepts a communication
27 from an external destination device to an application

1 transmitted through said network, verifies a digital
2 signature provided for a message document exchanged via said
3 communication, and transmits said message document that has
4 been authorized.

5 11. A network system comprising:

6 multiple groups connected to a wide area network, all
7 of which have applications for performing data processing
8 and proxy servers connected to said applications via a local
9 area network,

10 wherein said proxy server intercepts a communication
11 transmitted by an application of a local group to an
12 application of a different group, provides a digital
13 signature for a message document exchanged via said
14 communication, and transmits said message document with said
15 digital signature to said application of said different
16 group, and

17 wherein said proxy server intercepts a communication
18 from said application of said different group to said
19 application of said local group, verifies a digital
20 signature provided for a message document exchanged via said
21 communication, and transmits said authorized message
22 document to said application of said local group.

23 12. The network system according to claim 11, wherein, when
24 said application of said local group transmits a message
25 document, said proxy server stores the message document with
26 a digital signature in a log, and manages said log; wherein,
27 when said application of said local group receives a message
28 document from a different group, said proxy server stores in

1 a log a message document authenticated by a verification of
2 a digital signature, and manages said log; and wherein, at a
3 predetermined timing, said proxy server compares the
4 transmission log with the reception log for the same message
5 document, and authorizes communication.

6 13. The network system according to claim 12, wherein said
7 proxy server compares signature information for a digital
8 signature concerning the same message document.

9 14. The network system according to claim 12, wherein said
10 proxy server compares hash values used for providing a
11 digital signature for the same message document.

12 15. A digital signature method comprising: providing a
13 digital signature for a message document exchanged by
14 applications and for authorizing said message document,
15 including the steps of:

16 selecting, in accordance with the type of a message
17 document transmitted by a predetermined application, a key
18 used for providing a digital signature for said message
19 document;

20 providing a digital signature for said message
21 document, when key selection rules set for said key are not
22 established, by using a replacement key that is set in
23 advance for said key;

24 transmitting said message document with said digital
25 signature to a destination designated by said application;
26 and

27 using said key, when said key selection rules for said

1 key have been satisfied after said digital signature has
2 been provided using said replacement key, to again provide a
3 digital signature, and transmitting said message document
4 with said digital signature to said destination.

5 16. A digital signature verification method comprising: for
6 verifying a digital signature provided for a message
7 document exchanged by applications, and for authorizing said
8 message document, including the steps of:

9 accepting a message document with a digital signature
10 that uses a replacement key, when said digital signature on
11 said received message document has been provided by using
12 said replacement key for an original key that is determined
13 in accordance with the type of said message document;

14 receiving a message document, after said message
15 document signed using said replacement key has been
16 accepted, with a digital signature that used said original
17 key; and

18 verifying a digital signature, provided using said
19 original key, to authorize said message document with said
20 digital signature that uses said replacement key.

21 17. A storage medium on which input means of a computer
22 stores a computer-readable program that permits said
23 computer to function as:

24 key management means for managing a key used to
25 generate a digital signature to be provided for a message
26 document that is exchanged between said applications;

27 signature key determination means for extracting said
28 message document from a predetermined application, and for,

1 based on said message document, determining a key used to
2 provide a digital signature; and

3 signature generation means for providing a digital
4 signature for said message document by using said key that
5 is obtained from said key management means based on a
6 determination made by said signature key determination
7 means.

8 18. A storage medium on which input means of a computer
9 stores a computer-readable program that permits said
10 computer to perform:

11 a process for selecting a key used to provide a digital
12 signature for a message document in accordance with a type
13 of message document transmitted from a predetermined
14 application;

15 a process for providing said digital signature for said
16 message document using said key that is selected, and for
17 employing a predetermined replacement key to provide said
18 digital signature for said message document, when key
19 selection rules for said key used to provide a digital
20 signature for said message document have not been satisfied;
21 and

22 a process for employing said key to provide again a
23 digital signature for said message document, when said key
24 selection rules for said key are satisfied after said
25 digital signature has been provided using said replacement
26 key.

27 19. A program transmission apparatus comprising:

1 storage means for storing a program that permits a computer
2 to function as:

3 key management means for managing a key used to
4 generate a digital signature to be provided for a
5 message document that is exchanged between said
6 applications,

7 signature key determination means for extracting
8 said message document from a predetermined application,
9 and for determining a key used to provide a digital
10 signature based on said message document, and

11 signature generation means for providing a digital
12 signature for said message document by using said key
13 that is obtained from said key management means based
14 on a determination made by said signature key
15 determination means; and

16 transmission means for reading said program from said
17 storage means, and for transmitting said program.

18 20. A program transmission apparatus comprising:

19 storage means for storing a program that permits a
20 computer to perform:

21 a process for selecting a key used to provide a
22 digital signature for a message document, in accordance with
23 the type of message document transmitted from a
24 predetermined application,

25 a process for providing said digital signature for
26 said message document using said key that is selected, and
27 for employing a predetermined replacement key to provide
28 said digital signature for said message document when key

1 selection rules for said key used to provide a digital
2 signature for said message document have not been satisfied,
3 and

4 a process for, when said key selection rules for
5 said key are satisfied after said digital signature has been
6 provided using said replacement key, employing said key to
7 provide again a digital signature for said message document;
8 and

9 transmission means for reading said program from said
10 storage means, and for transmitting said program.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
3310
3311
3312
3313
3314
3315
3316
3317
3318
3319
33100
33101
33102
33103
33104
33105
33106
33107
33108
33109
33110
33111
33112
33113
33114
33115
33116
33117
33118
33119
331100
331101
331102
331103
331104
331105
331106
331107
331108
331109
331110
331111
331112
331113
331114
331115
331116
331117
331118
331119
3311100
3311101
3311102
3311103
3311104
3311105
3311106
3311107
3311108
3311109
3311110
3311111
3311112
3311113
3311114
3311115
3311116
3311117
3311118
3311119
33111100
33111101
33111102
33111103
33111104
33111105
33111106
33111107
33111108
33111109
33111110
33111111
33111112
33111113
33111114
33111115
33111116
33111117
33111118
33111119
331111100
331111101
331111102
331111103
331111104
331111105
331111106
331111107
331111108
331111109
331111110
331111111
331111112
331111113
331111114
331111115
331111116
331111117
331111118
331111119
3311111100
3311111101
3311111102
3311111103
3311111104
3311111105
3311111106
3311111107
3311111108
3311111109
3311111110
3311111111
3311111112
3311111113
3311111114
3311111115
3311111116
3311111117
3311111118
3311111119
33111111100
33111111101
33111111102
33111111103
33111111104
33111111105
33111111106
33111111107
33111111108
33111111109
33111111110
33111111111
33111111112
33111111113
33111111114
33111111115
33111111116
33111111117
33111111118
33111111119
331111111100
331111111101
331111111102
331111111103
331111111104
331111111105
331111111106
331111111107
331111111108
331111111109
331111111110
331111111111
331111111112
331111111113
331111111114
331111111115
331111111116
331111111117
331111111118
331111111119
3311111111100
3311111111101
3311111111102
3311111111103
3311111111104
3311111111105
3311111111106
3311111111107
3311111111108
3311111111109
3311111111110
3311111111111
3311111111112
3311111111113
3311111111114
3311111111115
3311111111116
3311111111117
3311111111118
3311111111119
33111111111100
33111111111101
33111111111102
33111111111103
33111111111104
33111111111105
33111111111106
33111111111107
33111111111108
33111111111109
33111111111110
33111111111111
33111111111112
33111111111113
33111111111114
33111111111115
33111111111116
33111111111117
33111111111118
33111111111119
331111111111100
331111111111101
331111111111102
331111111111103
331111111111104
331111111111105
331111111111106
331111111111107
331111111111108
331111111111109
331111111111110
331111111111111
331111111111112
331111111111113
331111111111114
331111111111115
331111111111116
331111111111117
331111111111118
331111111111119
3311111111111100
3311111111111101
3311111111111102
3311111111111103
3311111111111104
3311111111111105
3311111111111106
3311111111111107
3311111111111108
3311111111111109
3311111111111110
3311111111111111
3311111111111112
3311111111111113
3311111111111114
3311111111111115
3311111111111116
3311111111111117
3311111111111118
3311111111111119
33111111111111100
33111111111111101
33111111111111102
33111111111111103
33111111111111104
33111111111111105
33111111111111106
33111111111111107
33111111111111108
33111111111111109
33111111111111110
33111111111111111
33111111111111112
33111111111111113
33111111111111114
33111111111111115
33111111111111116
33111111111111117
33111111111111118
33111111111111119
331111111111111100
331111111111111101
331111111111111102
331111111111111103
331111111111111104
331111111111111105
331111111111111106
331111111111111107
331111111111111108
331111111111111109
331111111111111110
331111111111111111
331111111111111112
331111111111111113
331111111111111114
331111111111111115
331111111111111116
331111111111111117
331111111111111118
331111111111111119
3311111111111111100
3311111111111111101
3311111111111111102
3311111111111111103
3311111111111111104
3311111111111111105
3311111111111111106
3311111111111111107
3311111111111111108
3311111111111111109
3311111111111111110
3311111111111111111
3311111111111111112
3311111111111111113
3311111111111111114
3311111111111111115
3311111111111111116
3311111111111111117
3311111111111111118
3311111111111111119
33111111111111111100
33111111111111111101
33111111111111111102
33111111111111111103
33111111111111111104
33111111111111111105
33111111111111111106
33111111111111111107
33111111111111111108
33111111111111111109
33111111111111111110
33111111111111111111
33111111111111111112
33111111111111111113
33111111111111111114
33111111111111111115
33111111111111111116
33111111111111111117
33111111111111111118
33111111111111111119
331111111111111111100
331111111111111111101
331111111111111111102
331111111111111111103
331111111111111111104
331111111111111111105
331111111111111111106
331111111111111111107
331111111111111111108
331111111111111111109
331111111111111111110
331111111111111111111
331111111111111111112
331111111111111111113
331111111111111111114
331111111111111111115
331111111111111111116
331111111111111111117
331111111111111111118
331111111111111111119
3311111111111111111100
3311111111111111111101
3311111111111111111102
3311111111111111111103
3311111111111111111104
3311111111111111111105
3311111111111111111106
3311111111111111111107
3311111111111111111108
3311111111111111111109
3311111111111111111110
3311111111111111111111
3311111111111111111112
3311111111111111111113
3311111111111111111114
3311111111111111111115
3311111111111111111116
3311111111111111111117
3311111111111111111118
3311111111111111111119
33111111111111111111100
33111111111111111111101
33111111111111111111102
33111111111111111111103
33111111111111111111104
33111111111111111111105
33111111111111111111106
33111111111111111111107
33111111111111111111108
33111111111111111111109
33111111111111111111110
33111111111111111111111
33111111111111111111112
33111111111111111111113
33111111111111111111114
33111111111111111111115
33111111111111111111116
33111111111111111111117
33111111111111111111118
33111111111111111111119
331111111111111111111100
331111111111111111111101
331111111111111111111102
331111111111111111111103
331111111111111111111104
331111111111111111111105
331111111111111111111106
331111111111111111111107
331111111111111111111108
331111111111111111111109
331111111111111111111110
331111111111111111111111
331111111111111111111112
331111111111111111111113
331111111111111111111114
331111111111111111111115
331111111111111111111116
331111111111111111111117
331111111111111111111118
331111111111111111111119
3311111111111111111111100
3311111111111111111111101
3311111111111111111111102
3311111111111111111111103
3311111111111111111111104
3311111111111111111111105
3311111111111111111111106
3311111111111111111111107
3311111111111111111111108
3311111111111111111111109
3311111111111111111111110
3311111111111111111111111
3311111111111111111111112
3311111111111111111111113
3311111111111111111111114
3311111111111111111111115
3311111111111111111111116
3311111111111111111111117
3311111111111111111111118
3311111111111111111111119
33111111111111111111111100
33111111111111111111111101
33111111111111111111111102
33111111111111111111111103
33111111111111111111111104
33111111111111111111111105
33111111111111111111111106
33111111111111111111111107
33111111111111111111111108
33111111111111111111111109
33111111111111111111111110
33111111111111111111111111
33111111111111111111111112
33111111111111111111111113
33111111111111111111111114
33111111111111111111111115
33111111111111111111111116
33111111111111111111111117
33111111111111111111111118
33111111111111111111111119
331111111111111111111111100
331111111111111111111111101
331111111111111111111111102
331111111111111111111111103
331111111111111111111111104
331111111111111111111111105
331111111111111111111111106
331111111111111111111111107
331111111111111111111111108
331111111111111111111111109
331111111111111111111111110
331111111111111111111111111
331111111111111111111111112
331111111111111111111111113
331111111111111111111111114
331111111111111111111111115
331111111111111111111111116
331111111111111111111111117
331111111111111111111111118
331111111111111111111111119
3311111111111111111111111100
3311111111111111111111111101
3311111111111111111111111102
3311111111111111111111111103
3311111111111111111111111104
3311111111111111111111111105
3311111111111111111111111106
3311111111111111111111111107
3311111111111111111111111108
3311111111111111111111111109
3311111111111111111111111110
3311111111111111111111111111
3311111111111111111111111112
3311111111111111111111111113
3311111111111111111111111114
3311111111111111111111111115
3311111111111111111111111116
3311111111111111111111111117
3311111111111111111111111118
3311111111111111111111111119
33111111111111111111111111100
33111111111111111111111111101
33111111111111111111111111102
33111111111111111111111111103
33111111111111111111111111104
33111111111111111111111111105
33111111111111111111111111106
33111111111111111111111111107
33111111111111111111111111108
33111111111111111111111111109
33111111111111111111111111110
33111111111111111111111111111
33111111111111111111111111112
33111111111111111111111111113
33111111111111111111111111114
33111111111111111111111111115
33111111111111111111111111116
33111111111111111111111111117
33111111111111111111111111118
33111111111111111111111111119
331111111111111111111111111100
33111111111111111

1 computer readable program code means in said computer
2 program product comprising computer readable program code
3 means for causing a computer to effect the functions of
4 claim 10.

5 24. A computer program product comprising a computer usable
6 medium having computer readable program code means embodied
7 therein for a network system, the computer readable program
8 code means in said computer program product comprising
9 computer readable program code means for causing a computer
10 to effect the functions of claim 11.

11 25. An article of manufacture comprising a computer usable
12 medium having computer readable program code means embodied
13 therein for causing a digital signature method, the computer
14 readable program code means in said article of manufacture
15 comprising computer readable program code means for causing
16 a computer to effect the steps of claim 15.

17 26. An article of manufacture comprising a computer usable
18 medium having computer readable program code means embodied
19 therein for causing a digital signature verification method,
20 the computer readable program code means in said article of
21 manufacture comprising computer readable program code means
22 for causing a computer to effect the steps of claim 16.

23 27. A program storage device readable by machine, tangibly
24 embodying a program of instructions executable by the
25 machine to perform method steps for a digital signature
26 method, said method steps comprising the steps of claim 15.

1 28. A program storage device readable by machine, tangibly
2 embodying a program of instructions executable by the
3 machine to perform method steps for a digital signature
4 verification method, said method steps comprising the steps
5 of claim 16.